消耗品や付属機器向けに費用対効果に優れたセキュア認証 IC を

Xavier Bignalet

このブログ記事では、Microchip 社の費用対効果に優れたセキュア認証 IC が、お客様にとって脅威となるモデルに対処可能なセキュリティ機能をどのように提供できるかを紹介します。付属品の単体認証や、規制可能な付属機器のエコシステム構築、あるいは消耗品の偽造対策に関心のある方は、ぜひご一読ください。

消耗品と付属機器のエコシステム構築をターゲットとした費用対効果に優れたセキュア認証 IC

お客様の身の周りでは、セキュア認証プロセスが毎日行なわれています。例えば、E メールを送信する時、携帯電話を充電器に差し込む時、あるいは文書をプリントするなどの行為の背後で認証が行なわれています。

なぜ、消耗品および付属機器の認証が必要なのか？

消耗品および付属機器エコシステムに認証がどうして不可欠なのでしょうか？まず第一の理由は安全の為です。機器はその目的の応じて危険な機能を実行せねばならない場合がありますが、認証によってシステムが正規品であり、メーカーの意図した安全な動作を保証できます。もう一つの理由は、互換性です。システム内の全てのパーツが、お客様のブランドのものであれ、第三者のものであれ、エコシステムの制御は同じユーザーエクスペリエンスを伝えることを保証するのに、認証が極めて重要になります。

またユーザー・エクスペリエンスも認証が必要な理由です。お客様のファームウェアにある IP を通じて、お客様毎のユニークな製品体験を提供し維持することができます。上記全てが、収益の保護とお客様のブランドイメージに影響を及ぼします。

消耗品および付属機器のマーケットセグメント

消耗品および付属機器のテクノロジーは、多数のマーケットセグメントを網羅しています。医療分野では、このような製品は、ケーブル、呼吸管、センサー、カートリッジ、パッチなどの品目に見られます。消費者セグメントでは、化粧品、E シガレット、印刷用の製品に見られます。さらには、芳香材と Qi®1.3 ワイヤレス充電用の製品にも見られ、この両者は自動車用製品にも使われています。その他の自動車製品としては、相手先ブランド製品（OEM）あるいは第三者による NFC カードや電気自動車バッテリーが挙げられます。工業用の消耗品および付属機器アクセサリー/ディスポーザブルとしては、第三者によるアクセサリー、メンテナンスサービス、OEM によるエコシステム制御が挙げられます。e-モビリティのマーケットセグメントでは、e-バイクの NFC カード、バッテリー交換、バッテリー認証に見ることができます。データセンターの製品では、暗号制御された製造のための OEM または第三者によるカード認証に関係するテクノロジーに見ることができます。このように消耗品および付属機器のエコシステムはどこにでもあります。Microchip 社は、全てのマーケットセグメントの製品に対して認証を提供することが可能です。

高レベルのポートフォリオ

Microchip 社は、その認証ポートフォリオの中からいくつかの高レベルのセキュリティ製品を提供しております。半導体製品の中から **CryptoAuthentication™** (ATECC608) デバイス、**CryptoAutomotive™** (TA100) セキュリティ IC、**Trusted Platform Module (TPM)** (**ATTPM20P**) および **Platform Root of Trust** を提供しております。車内搭載品としては、**Trust Platform** を提供しており、これには Trust&GO、TrustFLEX、TrustCUSTOM があります。この 3 つの階層では、Microchip 社のセキュア プロビジョニング サービスを活用し、お客様がニーズに合うセキュア認証 IC を選択して、プロビジョニングしたい認証情報を選び、ご希望に最も適った最小発注量（MOQ）を選定できます。プラットフォームが、試作品から製造に至るまでの全過程を通してお客様をサポートいたします。

セキュア認証はどのように作動するのでしょうか？

セキュア認証 IC は、マイクロコントローラ（MCU）に対するコンパニオンデバイスです。これは、秘密を守る金庫のような役割を果たしています。

秘密情報(鍵、認証情報、データ)は、Microchip 社の安全な書き込み施設において、デバイス内のセキュアメモリに書き込まれます。秘密情報は、使用時のみならず書き込み時においても、このようにして外部に漏らさない取り扱いが必要となります。

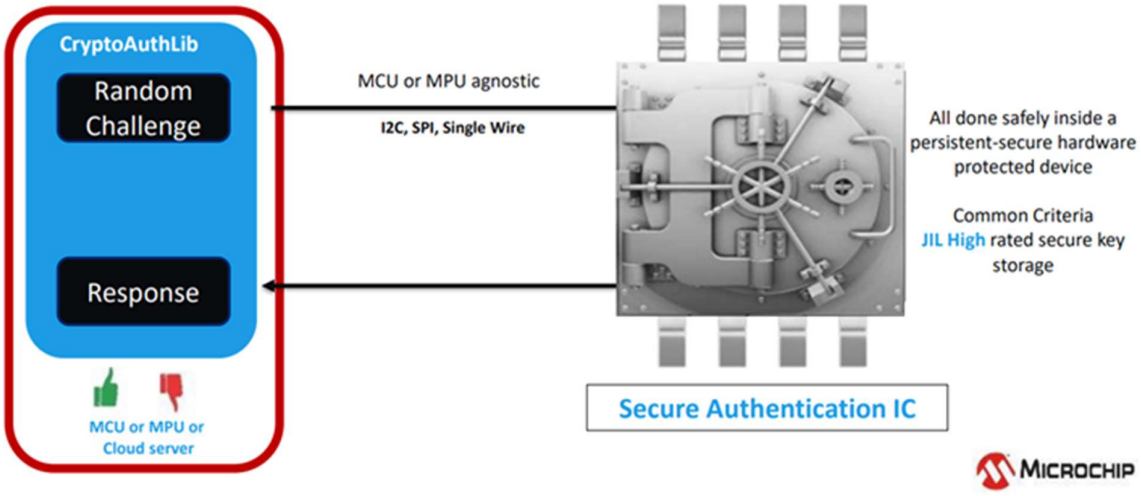

図 1：セキュア認証プロセス

ホスト MCU は、秘密鍵と暗号エンジンを持つセキュア認証 IC にランダムチャレンジを送信します。そのチャレンジは暗号エンジンに鍵とともに送り込まれ、認証用のレスポンスが生成されます。

ポートフォリオの拡張

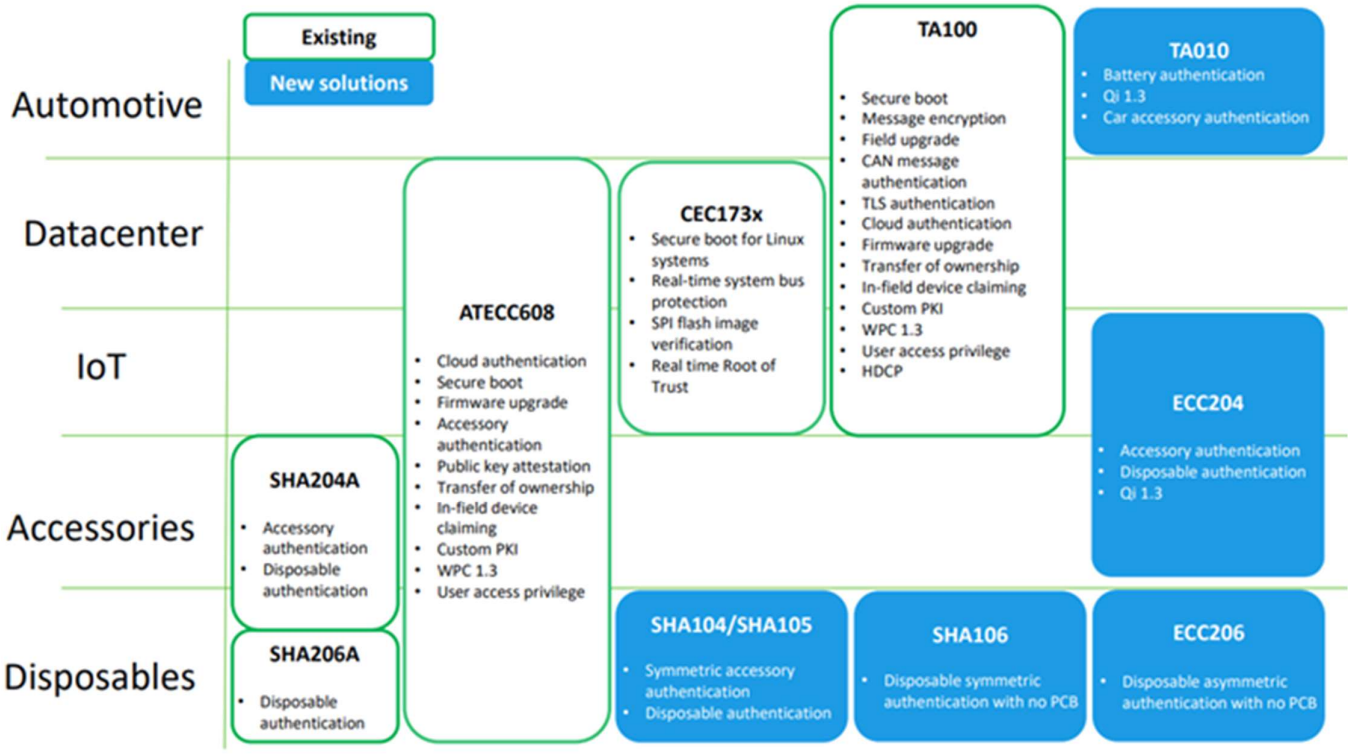

図 2：Microchip 社のポートフォリオ

最近 Microchip 社は、自動車市場用に TA010 を発売するなどポートフォリオにいくつかの新しいソリューションを追加しました。消耗品/付属機器については、SHA104/SHA105、SHA106 および ECC206 に加えて当社の新しい ECC204 をご覧ください。

このような新しいデバイスの設計意図は、コストの最適化を図るためにメモリ領域をコンパクトに保ち、最小限の実行可能な暗号アクセラレータを提供することにあります。従って、ECDSA 署名もしくは HMAC が上記のデバイスによってサポートされる暗号アルゴリズムとなります。さらに完全なアクセラレータを必要とする場合は、TA100 と ATECC608 をお勧めします。

対称認証

対称認証は、最も簡単な種類の認証で、ホストがクライアント（消耗品/付属機器）を認証するのに必要な秘密鍵が 1 つだけに限定されています。

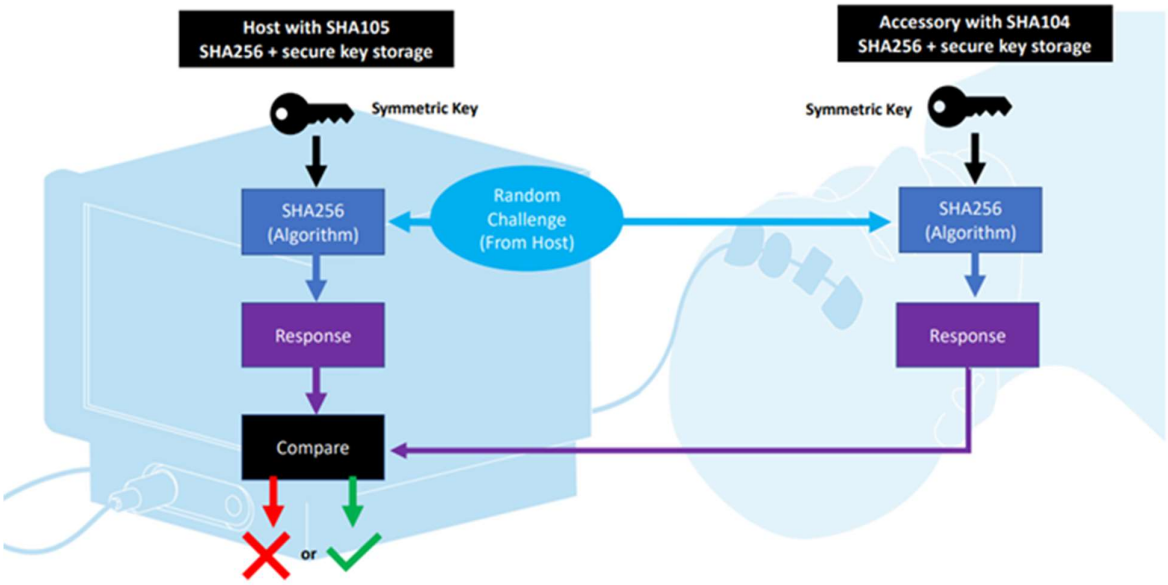

図 3：基本的な対称認証の原則

脳センサーとホストが描かれている上記の例をご覧ください。両側にセキュアなシステムがあります。左側には SHA105 が右側には SHA104 があります。ホストはセンサーにチャレンジを送信します。この時に両側では対称鍵が用いられます。双方でダイジェストまたはレスポンスを生成するのに SHA256 アルゴリズムを実行します。次に、消耗品/付属機器からのレスポンスがホストに戻されて、センサーからの情報を受け取るのに両方のレスポンスが同一であることが確認されます。

このプロセスを実行する最適な方法が、対称鍵の多様化です。この方法は各単一の消耗品/付属機器に対してユニークな対称鍵を提供する方法なので、各鍵の偽造のリスクおよびシステム全体が外部に暴露されるリスクが低減できます。

非対称認証

非対称認証、すなわち公開鍵暗号は、認証を行なうのに二種類の鍵（公開鍵と秘密鍵のペア）を使います。

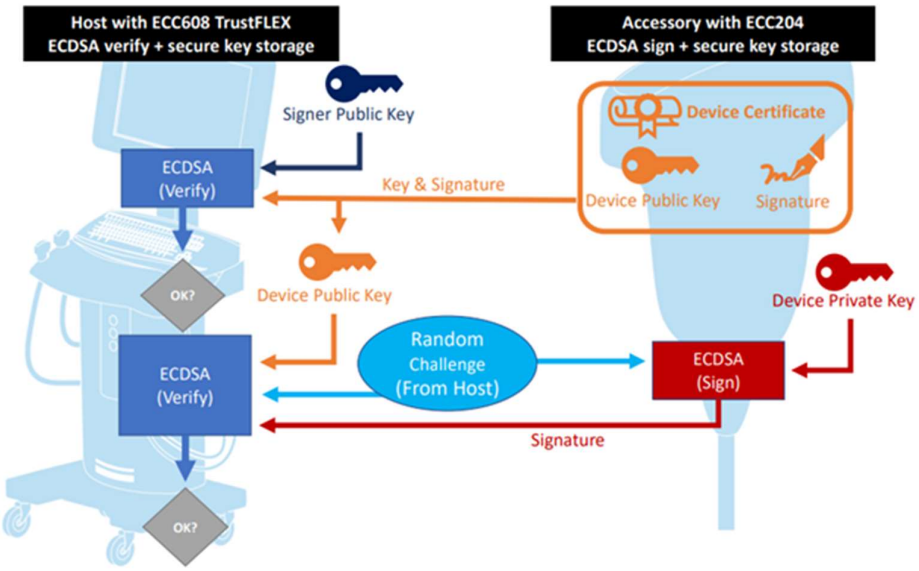

図 4：非対称認証

このシナリオでは（例えば、Qi 1.3 standard で行なわれるのに類似する方法で）クライアントとホストの間に認証が確立していると想定でき、組み込みシステムおよびチャレンジに対する応答がどのように行なわれているのかを見ることができます。署名者の公開鍵がホストに、デバイスの公開鍵が付属機器にあります。署名は、秘密鍵によってランダムチャレンジに実行される ECDSA 署名操作の出力です。デバイスの公開鍵は、署名者の公開鍵によって検証され、デバイスの公開鍵が署名の検証をします。次に、システムは操作を継続して、さらに情報を受け入れることができます。

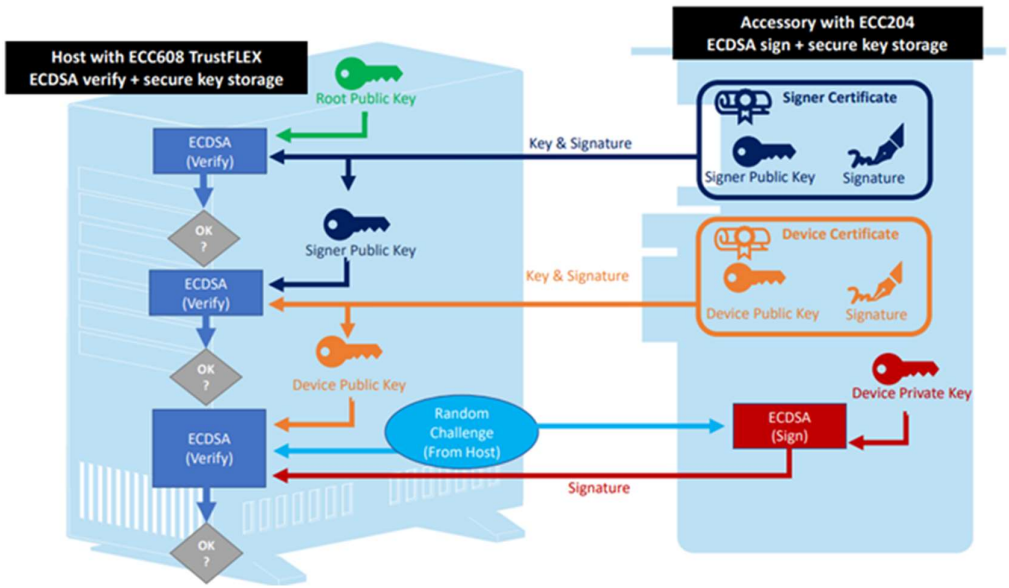

図 5：Root 公開鍵を使用した非対称認証

このシナリオは、root または OEM の公開鍵を加えているために多少複雑になっています。root による署名者の公開鍵から署名者によるデバイスの公開鍵までの各段階の公開鍵を検証し、さらに、署名が適正であることを認証する必要があります。システムが署名が正しいと認めると、システムが前に進めます。

寄生電源：3 ピンから 2 ピンに

寄生電源手法は、パッケージの中のピンの数を削減するのに極めて重要です。当社は、認証の計算を実行し応答を提供するのに十分なエネルギーを保持できる統合されたコンデンサーをデバイスの手前に追加しました。このコンデンサーの追加により電源ピンを削除した 2 ピンパッケージを実現しました。一本のピンには通信時にデータと電力が通っており、二本目のピンはグラウンドです。ピンの数が減少すると消耗品に PCB が必要なくなるために、システムレベルでのコストが低減し、実装の簡素化を図ることが可能になります。

セキュア 鍵 プロビジョニング サービス

当社の工場でマイクロチップにはハードウェア セキュリティ モジュール（HSM）が装備されています。この装備は、お客様とデバイスの間で暗号操作が行なわれるところに取り付けられます。当社は、様々なお客様から数多くのプロジェクトを引き受けて、機密にする必要のある鍵やその他のデータのプロビジョニングを行なうことができます。
概要は、こちらのページをご覧ください：**Trust Platform** 。

Trust Platform Design Suite

Microchip 社の **DM320118** は、**Trust Platform Design Suite (TPDS)** やその他のソフトウェアツールと一緒に使うことができるために、お客様が始めるのをサポートする時のベースキットとなっています。どのアドオンボードがお客様にとって適正であるのかをお確かめください。ソケット アドオンボードもご利用になれます。TPDS は、対称認証と非対称認証さらに Qi 1.3 のケーススチュートリアルの使用のためのアクセスを提供しています。TPDS は、C コードの例、選定されたセキュア認証 IC に対するコンフィギュレータ、マイクロチップ セキュア プロビジョニング サービスに実装するのに必要とされるユーティリティも提供しています。

結論

Microchip 社のポートフォリオは、お客様にセキュア認証への簡単なアクセス、簡単なツールセットを使用した迅速な開発、e コマースストアを活用したシンプルなフローを提供します。当社の製品は、**CryptoAuthLib** に捉われないプロビジョニングとアーキテクチャーを含めて、MoQ の低いマスマーケット向けの製品です。

セキュア認証について深く知るには当社の **Design Week 2023 session** をぜひご覧ください。
詳細については、**セキュア認証ウェブページ**をご覧ください。